REMARKS

The enclosed is responsive to the Examiner's Office Action mailed on February 10, 2009. At the time the Examiner mailed the Office Action, claims 1, 3-5, 7-17, 19, 21-24 and 27-30 were pending. By way of the present response applicants have: 1) amended claims 1, 7, 10, 16, and 19; 2) added no claims; and 3) canceled no claims. As such, claims 1, 3-5, 7-17, 19, 21-24 and 27-30 are now pending. No new matter has been added. Reconsideration of this application as amended is respectfully requested.

Examiner Interview

Applicants thank the Examiner for taking the time to participate in a telephonic interview on May 11, 2009 with the undersigned attorney for applicants. During the interview, the parties discussed the application of the references to the independent claims, specifically with reference to claim 1. The arguments set forth by the undersigned attorney for applicants during the interview are included below. No agreement regarding the patentability of the claims was made.

Claim Objections

The Examiner objected to claims 1, 7, 10 and 16 for various informalities. Applicants have amended claims 1, 7, and 16 to clarify the antecedent basis of certain terms. Claim 10, however, recites "data received by the portable data storage device." Applicants respectfully submit that this received data can be stored in the non-volatile memory and relate to "data" in line 2 of claim 1, but is not so limited and, therefore, is addressed separately. Additionally, in light of the claim

amendments, the references to "data" and "data received..." are more clearly stated. Accordingly, applicants respectfully submit that the objection to claims 1, 7, 10 and 16 has been overcome.

Claim Rejections – 35 U.S.C. §103

Claims 1, 3-5, 7-9, 11-13, 15-17, 19, 21-24 and 27-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brandys (WO 02/073877A2, hereinafter, "Brandys") in view of Buch (U.S. Patent Pub No. 2003/0217165 hereinafter, "Buch").

Brandys describes a smart card that verifies biometric information and digitally signs messages upon authenticating a user. In particular, Brandys describes that the smart card signs a message by hashing the message to create a message digest, which is then encrypted with a private key to create a digital signature. A recipient of the message can verify the signature by using a public key.

Buch describes user authentication of Session Initiation Protocol (SIP) messages using certificates. In particular, Buch describes an invite message containing a public key certificate to initiate a communication session in a computer network. The public key certificate is used to determine the identity of the sender and whether or not the communication request is accepted.

Applicants respectfully submit that Brandys does not teach or suggest a combination with Buch and that Buch does not teach or suggest a combination with Brandys. The combination of Brandys and Buch is the result of impermissible hindsight based solely upon the present application.

Even if Brandys and Buch were combined, the combination fails to disclose all of the features of claim 1. For example, the combination fails to disclose a secret key that is permanently stored in the portable storage device, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key. Applicants note that the present application differentiates between a private key generated by an integrated circuit and a secret key that is permanently stored within the device. (see, e.g., Specification, page 3, lines 13-15, and page 8, lines 1-28). Brandys describes that a private key is created when the smart card receives biometric data from a user, but is silent regarding permanently storing a secret key in a portable storage device. (Brandys, page 3, line 35 to page 4, line 1). Similarly, Buch describes the user generating a pair of public and private keys, not a secret key that is permanently stored in a portable storage device. (Buch, paragraph [0033]).

Additionally, the combination fails to disclose the host requesting the data stored in the non-volatile memory, the data stored prior to receiving the command, and the portable data storage device to transmit the encrypted key and the requested data stored in the non-volatile memory to the host. The Office Action asserts that Brandys discloses this claim feature in that "the smart card receives biometric data from a user (i.e. request), the public key is transmitted (page 3, line 3, page 4, lines 1-4). Brandys also discloses that non-volatile memory of the smart card stores information such as the public key (page 7, lines 8-12)." (Office Action dated 2/10/09, page 3). Applicants respectfully submit that the interpretation of a smart card receiving biometric data as being equivalent to a request for data stored in the non-volatile memory is unreasonably broad. In contrast to this interpretation,

Brandys discloses that the receipt of biometric data "triggers the random number generator 204 **to create** a public key 220 and a private key 224." (Brandys, page 4, lines 1-2) (emphasis added).

Furthermore, the claim 1 differentiates between a key and the requested data – both are transmitted to the host – therefore, the requested data should be treated separately and as different from the key. The Office Action's allegation that the public key is the requested data fails to read the claim as a whole. Brandys describes a non-volatile memory that can store the private key, biometric measurement templates, the public key, a card serial number, a personal identification number, biometric standards or limits, authorization limits, etc. (Brandys, page 7, lines 11-13). Applicants, however, submit that Brandys is silent about any of these things being data that is requested by a host.

Instead, Brandys is focused on signing a message: Brandys describes **receiving a message**, creating a digital signature, and transmitting the digital signature appended to the message. (Brandys, page 4, lines 17-23). The message in Brandys is received – i.e., it is not data that was stored prior to the request or command. Furthermore, Brandys describes creating a digital signature using a key and transmitting the signature. Applicants respectfully submit that a digital signature is not the equivalent of a key, as alleged by the Office Action (see, e.g., Brandys pages 5-6). Brandys does not disclose encrypting the generated key using a secret key. Instead, as stated above, Brandys describes generating a signature using a private key.

Buch describes using public key certificate to determine the identity of the sender of an SIP message and whether or not the communication request is

accepted. Buch is silent regarding a host requesting the data stored in the non-volatile memory of a portable data storage device and the portable data storage device to transmit an encrypted key and the requested data stored in the non-volatile memory to the host.

The combination also fails to disclose the portable data storage device is arranged **to receive from the host a digital signature based on the generated key and the requested data** transmitted to the host from the portable storage device, the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host. The Office Action alleges that Buch discloses this claim feature in paragraph [0028]. Applicants respectfully submit that the citation relied upon by the Office Action only discusses decrypting the digital signature of the sender and generating hash values to authenticate the key used to generate the signature, it is silent regarding receiving, from the host, a digital signature based on the generated key and the requested data sent to the host.

For example, based upon the assertion of Buch by the Office Action, the caller is sending an invite request to a callee. Buch, however, merely discloses that the callee is able to determine that a particular request message has been sent from the caller based on the signature in the request message. Buch does not disclose that the caller is able to use any received signature from the callee to verify that requested data has been correctly received by the callee. Instead, Buch merely describes that the verification of a digital signature results in the callee sending an "OK message" to the caller. (Buch, paragraph [0045]). An OK message, e.g., a standard handshaking protocol, is distinct from a digital signature.

Applicants respectfully submit that both Bradys and Buch are concerned with transmitting a digital signature in a single direction. Bradys describes a smart card that creates a digital signature and sends it to another device. Buch describes an SIP device ("caller") sending a digital signature to another SIP device ("callee"). Neither the smart card of Brandys nor the caller SIP client of Buch receives any digital signature, much less a digital signature based on the at least one generated key and the requested data sent by the smart card/caller to verify that the requested data has been correctly received by another device/callee.

Accordingly, applicants respectfully submit that the rejection of claim 1 in view of Brandys and Buch has been overcome. Given that independent claims 16 and 19, while different from claim 1, contain features similar to claim 1 as discussed above, applicants respectfully submit that claims 16 and 19 are patentable over Brandys and Buch for at least the same reasons as above.

Given that claims 3-5, 7-15, 17, 21-24, and 27-30 are dependent claims with respect to claims 1, 16, and 19, and include additional features, applicants respectfully submit that claims 3-5, 7-15, 17, 21-24, and 27-30 are patentable over Brandys and Buch for at least the same reasons as above.

Claims 10 and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brandys in view of Buch as applied to claims 1 and 19, and further in view of Iwagaki et al., (U.S. Patent Pub No. 2003/0161468 A1 hereinafter, "Iwagaki").

Claims 10 and 30 are dependent upon claims 1 and 19 respectively. Applicants respectfully submit that Iwagaki does not remedy the shortcomings of

Brandys and Buch as discussed above. Accordingly, applicants respectfully submit that the rejection of claims 10 and 30 in view of Brandys, Buch, and Iwagaki has been overcome.

Claim 14 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Brandys in view of Buch as applied to claim 1, and further in view of Fang, (U.S. Patent 6,536,941 hereinafter, "Fang").

Claim 14 is dependent upon claim 1. Applicants respectfully submit that Fang does not remedy the shortcomings of Brandys and Buch as discussed above. Accordingly, applicants respectfully submit that the rejection of claim 14 in view of Brandys, Buch, and Fang has been overcome.

CONCLUSION

Applicants respectfully submit that in view of the amendments and arguments set forth herein, the applicable objections and rejections have been overcome. Applicants reserve all rights under the doctrine of equivalents.

Pursuant to 37 C.F.R. 1.136(a)(3), applicants hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. 1.16 and 1.17, to Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: May 11, 2009

/Ryan W. Elliott/
Ryan W. Elliott
Reg. No. 60,156

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300